A Novel Architecture for Information Security using Division and Pixel Matching Techniques

Abdulrahman Abdullah Alghamdi
College of Computing and IT, Shaqra University
Kingdom of Saudi Arabia

***Abstract*—The computer users have to safeguard the information which they are handling. An information hiding algorithm has to make sure that such information is undecipherable since it may have some sensitive information. This paper proposes a steganography method that conceals the message behind the image by providing the security when compared to the other existing methods. In this system, the information to be hidden is encrypted by an advanced cryptography technique. For that, initially, the data is divided by the method of arithmetic division. The information is hold on within the style of the divisor, the quotient and the remainder. The secret key is also encrypted and holds on several pixels. Then, the pixel matching algorithm is used to hide the information of the secret image in the carrier image. By this system, the embedding time is reduced when compared to different existing algorithms. In this method, different types of images are used for testing the proposed algorithm. By using this method, the peak signal to noise magnitude relation obtained is more for all the pixels present in the image.**

Keywords—Information security; steganography; pixel pattern matching; key segmentation; division method

I. Introduction

Steganography is the science of computing that hides the secret data inside a carrier image. Steganography [5, 6, 13, 15] is an information hiding activity proposed in recent years. Image steganography is most often associated with information hiding which includes the process of hiding important information in a secret image. This can be sometimes done by the replacement of pixels that is necessary bits of data which is present inside the carrier image, [11] where the Cryptographic methodology separates the message into different parts. Based on its priority, it hides the message. Image steganography works on all types of information present in an image to hide it into another image. Audio and Video Steganography are the other two types of techniques that can be a used to hide any information into a hidden video or audio file [12].

The encoded information called as the cipher text is unclear so that the hacker cannot find it. Cryptography provides data security by applying encryption/decryption techniques. The purpose of Image steganography is to upgrade the safe transmission of data by concealing different data files into concealing image and to prevent an adversary from extracting the data [14]. A novel image steganography approach has been proposed in [1] which uses Fuzzy Inference System (FIS) in Mamdani type with the Human Visual System (HVS) properties. Authors in [2] proposed that the secret data is transformed into fuzzy domain. Two image processing techniques like edges and texture are exploiting for fuzzy pixel. LSB steganography substitution is used for embedding and obtained high imperceptibility. Acceleration of LSB Algorithm in GPU [3] presents a method for accelerating the steganography using Computer Unified Device Architecture (CUDA) by parallelizing the computations to a single pixel with a hybrid of message passing [7] and shared memory thereby reducing the runtime of the program. Authors in [4] Proposes the secret data is encrypted using fuzzy technique to increase the hidden robustness.

II. Literature Survey

The steganography-based information hiding can be categorized in to transform based and domain-based methods [10]. In the transform-based method, the data is encoded initially and then it is hidden within the cover image. The transform-based method hides messages in additional areas of the image. This initiates the cover image to separate in to priority-based techniques such as high, middle and low. The foremost important character of this strategy is, this method is best against various attack in images. In the Domain based strategies, messages are encoded within the intensity of the pixels. Least-significant bit (LSB) [11, 12] is an example of the domain-based techniques.

Xu et al [8] developed a novel method for steganography using the hybrid-based edge detector technique. Their technique uses the combination of character detection methodology and edge detection algorithms. This methodology overcomes the existing methods for steaganalysis systems. It additionally generates the prime quality stego pictures. Every steganography-based technique has its own disadvantages. Petitcolas et al [10] proposed a methodology which overcomes the various disadvantages of already used steganography systems. Modification of information in an image medium is termed as steganographic attacks. These are often delineated in several forms that can be predicated on numerous techniques of knowledge concealment. Cheddad et al in [11] elaborates three kinds of steago attacks particularly attacks in hardiness, attacks in presentation, and attacks in interpretation.

From the works found in the literature, it's been ascertained that most of the prevailing works used threshold based algorithms; fuzzy c means algorithm s and neural networks-based algorithms. However, just in case of medical applications, the accuracy provided by numerous phases of segmentation isn't enough to form effective selections. Also, it has been observed that most of the existing methods show less accuracy in hiding the images which has more information. Therefore, a new and efficient methodology to embed the most important messages in a carrier image more effectively is necessary.

III. Proposed Methodology

The Combination of Division method and pixel matching methodology is proposed for embedding the most important information as an image in to a carrier image. This combination makes an effective process of steganography even the secret information is of more quantity since it is based on the pixels.

A. Division Method

The secret image is given as input to this process. Then, it's transformed towards the decimal worth with the assistance of an ASCII code, which can further as a dividend. A random value is formed which is considered as a divisor. Then, the mathematical operation called as the division is done using both the values obtained from the dividend and divisor method. The equation for performing the division method is as follows:

$$M = D*Q+R \tag{1}$$

Where D is the Divisor, Q is the quotient, R is the Remainder and M is the secret message which is to be hidden in the carrier image.

B. Pixel Matching Technique

The Pixel matching [9] is used for hiding the secret knowledge into the frames of an image file. In this process, the secret data is hidden into the carrier image and it will not change the properties of the carrier image [10]. The Pixel matching process is as follows. Four matching rules where written for this method. This method compares the pixels of original and secret pictures and hides the key image generated from the division methodology within the original image. All the matching rules begin the iteration from the initial pixel of the original image and with the secret image

Matching Rule 1: If the pixel in the Carrier image is Black and the pixel in the Secret image is White then, go to the next pixel in the original image.

Matching Rule 2: If the pixel in the Carrier image is black and the pixel in the Secret image is black, then insert the value of M computed through the division method and merge the pixel of the secret image with the original image. After merging, go to next pixel in both images.

Matching Rule 3: If the pixel in the Carrier image is white and the pixel in the Secret image is black, then go to the next pixel in the secret image.

Matching Rule 4: If the pixel in the Carrier image is white and the pixel in the Secret image is white, then insert the value of M computed through the division method and merge the pixel of secret image with the original image. Continue the process for the complete image.

C. Division based Pixel Matching

In this work, a completely unique approach of combining the division method, Pixel grouping and matching algorithmic rule is developed. In this work, the image is scanned from the first pixel to the last pixel. Initially, the set of eight pixels are taken into consideration. Here, the matching rules are applied to check whether the pixel is a grey or black and to combining the calculated M value with the division method. Since the image is converted into grey scale, it has only black and grey pixels. Repeat the process until all the complete pixels are computed and changed. The proposed algorithm for Fuzzy based pixel grouping and matching is shown below

```
Step.1 Set $R_1$ = First eight pixels,
Step.2 if $R_C$= black and $R_S$ = white
Step 3 Go to the next pixel
Step 4if $R_C$= black and $R_S$ = black
Step 5 Insert the value of M and merge the pixels
Step.6 $R_C$= White and $R_S$ = black
Step 7 Go to the next pixel
Step 8 if $R_C$= White and $R_S$ = White
Step 9 Insert the value of M and merge the pixels
Step.10 Repeat the process till last pixel
Step 11. Continue step 2 if $R_1$ becomes ninth pixel
Step.12 End
```

D. Decoding Technique

Decoding is the process of receiving the hidden data from the carrier image. Initially, the proposed system retrieves the secret message from the user. In order to produce additional security, this encrypted secret message is more processed using the division method using the Quotient, Divisor and Remainder method. The system currently asks the user for the hidden output as information. When the user provides this information, the decoding technique reverses the process of division and the output is given towards the reverse of pixel matching technique which is the defuzzification process. From this technique, the hidden data is revealed along with the carrier image.

IV. Result and Discussion

This methodology is developed using MATLAB V10. The results were obtained by giving the secret image along with the carrier image. From the result obtained, it can be noticed that the proposed methodology provides a higher accuracy in hiding the information in a carrier image. This can be obtained from the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE). The MSE and the PSNR are the metrics used for scrutinizing the quality of a picture. In general, if the PSNR is higher, then the quality of processed image is also more. MSE is that the accumulative square error that lies between the processed and the original image. Once the MSE is low, then the error is also low. These parameters are calculated as follows

$$PSNR = 10\ log_{10}(R^2/MSE\ ) \tag{2}$$

TABLE I. ACCURACY BASED ON PSNR AND MSC

Image	PSNR (Existing method)	MSE (Existing method)	PSNR (Proposed method)	MSE (Proposed method)
Image 1	63.0288	0.1176	67.1268	0.1044
Image 2	69.0198	0.1084	72.0918	0.0190
Image 3	71.1187	0.2217	72.0435	0.1106
Image 4	67.0198	0.1196	64.4101	0.0293
Image 5	68.0139	0.2164	69.8731	0.1142

TABLE II. EXECUTION TIME TAKEN FOR THE DIFFERENT TYPES OF IMAGES WITH AND WITH OUT DIVISION OPERATOR (IN SECONDS)

Secret Image	No Division Operator	With Division Operator
	Time Taken for Existing Method (In Seconds)	Time Taken for Proposed Method (In Seconds)
Image 1	468	547
Image 2	353	629
Image 3	666	827
Image 4	659	582

Where, M and N are the number of rows and columns in the input images. Then the algorithm calculates the MSC value using the below equation.

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M*N} \quad (3)$$

Table 1 presents the accuracy obtained from the PSNR and MSE values for the steganographic output. The projected methodology is compared with existing steganography method. The results ascertained reveals that, this technique offers higher performance than the existing technique based on PSNR and MSE values.

Time taken (in seconds) for testing the images of same size is shown in Table 2. Method with division operator and with out division operator where taken for calculating the time complexity.

Table 1 exhibits the outcomes of the proposed system for information hiding. The accuracy estimation is based on the metrics such as PSNR and MSC. The type of image is delineated by the primary column. The succeeding column depicts the existing methodology for hiding the secret information in a carrier image. Similarly, Table 2 depicts the outcomes of the execution time in seconds considered for the different types of images with and without division operator respectively. The time taken for an existing method without the division operator is delineated in the primary column. The succeeding column depicts the time taken for the proposed method with division operator. From the results obtained it can be projected that the proposed system provides higher outcomes than the previous methods of information hiding.

V. CONCLUSION

The proposed methodology focuses on hiding the secret message in a carrier image by the process of combining the pixel matching and division operator. Hence, a hacker cannot guess and find the presence of the message which is hidden. This process successively increases the protection of secret information in the carrier image. Also, distortion is discovered within the systems wherever encrypting methodology called as LSB is employed. Therefore, the combination of pixel matching and division based methods keeps the secret data safer. The projected system uses the component based Pixel Matching together with the division method. This combination can be a secured system for hiding the secret messages so that the intruders cannot be able to acquire the hidden data. Hence, the projected methodology provides an interesting approach of information hiding in images. Future work can be a proposal of combination of algorithms to hide different types of secret information more accurately regardless of the size of the data.

REFERENCES

[1] Soleimanpour, “A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain”Iranian Journal of Electrical & Electronic Engineering, Vol. 9, No. 2, 2013.

[2] Silman J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001.

[3] Lee Y. K. and Chen L. H., “High capacity image steganographic model”, IEEE Proceedings ofVisual Image Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.

[4] Ker A., “Improved detection of LSB steganography in grayscale image”, Lecture Notesin Computer Science, pp. 97-115, 2005.

[5] Mahdavi, Samavi Sh., Zaker N. &MHashemi, “Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram”, Iranian Journal of Electrical& Electronic Engineering, Vol. 4, No. 3, pp. 59-70, 2008.

[6] Joan Daemen, Vincent Rijmen, “The Block Cipher Rijndael”, LNCS-CARDIS '98, 1998.

[7] Abdulrahman Abdullah Alghamdi, “Computerized Steganographic Technique using Fuzzy Logic”, International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018.

[8] Xu H., Wang J. and Kim H. J., “Near-optimal solution to pair-wise LSB matching via an immune programming strategy”, Information Sciences, pp. 1201-1217, 2010.

[9] R.Harralick, K.Shanmugam, Dinstein, “Textural Features for Image Classification”, IEEE Trsans on System, Man and Cybernetics, Vol 3, No 6, 1973, pp-610-621.

[10] Petitcolas F.A.P.,“Introduction to information hiding,” In: Katzenbeisser S., Petitcolas F.A.P. (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000.

[11] Cheddad A., Condell J., Curran K., and Mc Kevitt P., “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol.90, pp.727-752, 2010.

[12] Ms. Fameela. K. A, Mrs. Najiya. A and Mrs. Reshma. V. K, “Survey on Reversible Data Hiding in Encrypted Images”, International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 3, Issue 4, April 2014.

[13] S. Arora, S. Anand, “A proposed method for image Steganography using Edge Detection”, International Journal of Engineering technology and Advanced Engineering, Vol.3, Issue 2, February 2013.

[14] Vipula Madhukar Wajgade and Dr. Suresh Kumar, “Enhancing Data Security using Video Steganography”, International Journal of Emerging Technology and Advanced Engineering (IJETAC), Vol. 3, Issue 4, April 2013.

[15] Abdulrahman Abdullah Alghamdi, Information Security using Steganographic Method: Genetic Algorithm and Texture Features, Indian Journal of Science and Technology, Vol 11(34), 2018.